HN

UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/932,298	08/17/2001	Christina Fu	SUN-P6043	4864

			EXAMINER
7590	03/07/2005		SCHUBERT, KEVIN R

Jonathan P Osha
OSHA & MAY LLP
1221 McKinney Street
Suite 2800
Houston, TX 77010

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/932,298	FU, CHRISTINA
	Examiner	Art Unit
	Kevin Schubert	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _17 August 2001_.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-24_ is/are pending in the application.
   4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) _1-24_ is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on _17 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.
   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a)☐ All   b)☐ Some * c)☐ None of:
   1.☐ Certified copies of the priority documents have been received.
   2.☐ Certified copies of the priority documents have been received in Application No. _____.
   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.
4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

DETAILED ACTION

Claims 1-24 have been considered.

Claim Rejections - 35 USC § 112

5   Claim 6 recites the limitation "said cluster of servers". There is insufficient antecedent basis for

this limitation in the claim. The examiner assumes the applicant meant "said clone servers". Appropriate

correction is required.

Claim Rejections - 35 USC § 103

10   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
15 > invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4,8,12-18, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over

20   Zubeldia, U.S. Patent No. 6,044,462, in view of the applicant's admitted prior art.

As per claim 1, the applicant describes a method of creating a certificate revocation list

comprising the following limitations which are met by Zubeldia in view of the applicant's admitted prior art:

a) creating a single CRL that is centralized, said single CRL associated with a certificate authority

25   (CA) comprising a master server coupled to a plurality of CA clone servers (Col 7, lines 38-40; Fig 6);

b) maintaining said single CRL with said master server (Col 7, lines 14-15; Fig 6);

c) receiving notice, from one of said plurality of CA clone servers, at said master server

containing revocation information regarding a certificate (Col 7, lines 7-11);

d) updating said single CRL according to said revocation information (Col 7, line 66 to Col 8, line

30   7);

Zubeldia describes a system which eliminates the need for multiple CRL lists by maintaining a central database which stores validity information about certificates within a system. The central database maintains a list of all certificates that have been revoked as well as additional information about revoked certificates such as the data and time they were revoked (Col 8, lines 1-7). Additional

5   information, such as if a certificate has been reinstated, can also be stored in the database.

Zubeldia describes all the limitations of the above claim except for the limitation that the system takes place with CA clone servers. Zubeldia's system takes place with regular CA servers. As stated in the applicant's admitted prior art, a CA cluster is a CA which is comprised of CA clone servers which help manage the CA workload by dividing the certificates the CA manages amongst the CA clone servers

10   (applicant: Fig 2).

Zubeldia also discloses the idea that his system can be used on an individual CA for it to store the validity information of its own certificates (Col 7, lines 42-45). If Zubeldia's system takes place on an individual CA and the CA is a cluster with CA clones, it would not only be obvious to implement the applicant's system, it would be necessary because the CA clones would need to feed their certificate

15   statuses and/or CRLs to the server for storage in the database. Combining the idea of a CA cluster disclosed in the applicant's admitted prior art with the ideas of Zubeldia, a system is produced where the CAs of Zubeldia's system are replaced by CA clones. In this case, CA 602A, CA 602B, and CA 602C of Fig 6 of Zubeldia would be replaced with CA Clone 410, CA Clone 420, and CA Clone 430 of applicant's Fig 4. As one can see from the two figures, the systems parallel each other.

20   It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of the applicant's admitted prior art with those of Zubeldia and incorporate the use of CA clones instead of CAs because both systems accomplish the same goal of reducing a plurality of CRLs to maintain a central database of certificate validity information.

25   As per claims 2,14, and 17, the applicant describes the method of claims 1,12, and 16, which are met by Zubeldia in view of the applicant's admitted prior art, with the following limitation which is met by Zubeldia:

Wherein step d) comprises adding said certificate to said single CRL when said revocation

information indicates said certificate is revoked, said revocation information associated with a revocation

event occurring at one of said plurality of CA clone servers (Col 7, line 66 to Col 8, line 7).

5   As per claims 3,15, and 18, the applicant describes the method of claims 1,12, and 16, which are

met by Zubeldia in view of the applicant's admitted prior art, with the following limitation which is met by

Zubeldia:

Wherein step d) comprises removing said certificate from said single CRL when said revocation

information indicates said certificate is valid, said revocation information associated with a revocation

10   event occurring at one of said plurality of CA clone servers (Col 7, line 66 to Col 8, line 7);

The applicant should note that when a clone server reports that a certificate is valid, or reinstates

a certificate, the certificate is removed from revoked status and thus disassociated with a list of revoked

certificates in the database but still maintained in the database to provide information that the certificate is

valid.

15   Also, in another embodiment the CA clone servers submit CRLs to the database to maintain the

single CRL (Col 7, lines 10-11). If this is the case and a certificate become valid, it is removed from the

locally generated CRL and therefore removed from the central CRL when the locally generated CRL gets

to the database. Also, if the CA clone servers only submit locally generated CRLs, the database would

only contain information about revoked certificates, not information about valid certificates as well.

20

As per claims 4 and 21, the applicant limits the method of claims 1 and 16, which are met by

Zubeldia in view of the applicant's admitted prior art, with the following limitation which is met by Zubeldia:

Maintaining said single CRL with a CRL merger service module located at said master server

(Col 7, lines 14-15);

25   The CRL merger service module is the unit in charge of maintaining the database. The entire

server of Zubeldia can be thought of as the CRL merger service module.

As per claims 7 and 13, the applicant limits the method of claims 1 and 12, which are met by Zubeldia in view of the applicant's admitted prior art (see above), with the following limitation which is met by Zubeldia:

Transmitting said single CRL that is updated to a recipient over a communication network (Col 7, lines 29-37; Col 6, lines 57-59);

Referring to figure 6, a user requests information through a server which communicates with the database and sends the requested information back to the user. The requested information can be a validity check or a CRL (Col 6, lines 57-64).

As per claim 8, the applicant limits the method of claim 1, which is met by Zubeldia in view of the applicant's admitted prior art (see above), with the following limitation which is met by Zubeldia:

Providing certificate authority services not including maintaining and managing said single CRL at each of said plurality of CA clone servers (Col 7, lines 7-11).

The single CRL, which is the list of all revoked certificates in the database, is a maintained and managed by the server. All the CAs in Zubeldia's system function as normal CAs (Col 7, lines 7-11) with the exception that the CAs in Zubeldia's system do not maintain CRL lists but rather feed their generated CRL lists to the central database which maintains one CRL list for the system.

As per claims 12 and 16, the applicant discloses a method for generating and maintaining certificate revocation list information comprising the following limitations which are met by Zubeldia in view of the applicant's admitted prior art:

a) each of said clone servers independently generating revocation information relating to certificates (Col 7, lines 7-11);

b) sending said revocation information to a master server coupled to said plurality of clone servers (Col 7, lines 7-11);

    c) maintaining a single centralized certificate revocation list (CRL) based on said revocation information from said plurality of clone servers, said step c) performed by said master server (Col 7, lines 38-40);

    Zubeldia discloses all the limitations of the above claim except Zubeldia discloses CA servers instead of CA clone servers. Reasons for combining the applicant's admitted prior art disclosure of a CA cluster with Zubeldia are given in the rejection for claim 1.

    Claims 5,10,11, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zubeldia in view of the applicant's admitted prior art in further view of Parkvall, U.S. Patent Application Publication No. 2002/0080719.

    As per claims 5 and 19, the applicant limits the method of creating a CRL as described in claims 1 and 16, which are met by Zubeldia in view of the applicant's admitted prior art (see above), with the following limitation which is met by Parkvall:

    Sending said notice over a secure communications channel (Parkvall: [0004]);

    Zubeldia in view of the applicant's admitted prior art discloses all the limitations of the independent claims. However, neither Zubeldia nor the applicant discloses sending information over a secure communications channel.

    Parkvall discloses the notion of Stop and Wait ARQ communication between two parties in which one packet is sent to a recipient and the sender waits for an acknowledgement before sending a second packet. Thus, Parkvall introduces the idea of creating a secure communications channel through acknowledgement signals between a sender and a receiver. Parkvall's communication disclosure could be implemented on Zubeldia in view of the applicant's admitted prior art in which the CA clones communicate with the server through the secure communication method.

    It would have been obvious to one of ordinary skill in the art at the time the invention was filed to incorporate the ideas of Parkvall with those of Zubeldia in view of the applicant's admitted prior art to

create secure communication between the CA clones and the server so that a hacker does not

compromise security within the system.

As per claim 10, the applicant discloses the method of claim 1, which is met by Zubeldia in view

5   of the applicant's admitted prior art (see above), with the following limitation which is met by Parkvall:

a) at said one of said plurality of clone servers, detecting whether said notice was received at said

master server (Parkvall: [0004]);

b) repeatedly sending said notice until received by said master server (Parkvall: [0004]);

Through Stop and Wait Automatic Response Request (ARQ), an acknowledgement is sent to the

10   sender or clone server if the message is received (part a). Automatic Response Request also includes

sending a notice to repeat the sending of the message in the case of an error (part b).

As per claim 11, the applicant discloses the method of claim 10, which is met by Zubeldia in view

of the applicant's admitted prior art (see above), with the following limitation which is met by Parkvall:

15   Storing said notice if said notice was not received at said master server (Parkvall: [0004]);

Through Stop and Wait Automatic Response Request (ARQ), the message or packet is stored

until confirmation that it has been correctly received at which time the message or packet is deleted.

Claims 5,6,9,19,20, and 22-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over

20   Zubeldia in view of the applicant's admitted prior art in further view of Oracle (Oracle Internet Directory

Administrator's Guide. Release 2.0.6. 1999).

As per claims 5,6, and 19, the applicant describes the method of creating a CRL as described in

claims 1 and 16, which are met by Zubeldia in view of the applicant's admitted prior art (see above), with

25   the following limitation which is met by Oracle:

Sending said notice over a secure communication channel (Page 3);

Zubeldia in view of the applicant's admitted prior art discloses all the limitations of the

independent claims 1 and 16. However, neither Zubeldia nor the applicant discloses sending information

over a secure communication channel.

Oracle discloses the Oracle Internet Directory, a service which provides directory access control.

5   Among the features of Oracle Internet Directory are providing a secure communication channel through a

secure socket layer (SSL) authenticated access system.

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

combine the ideas of Oracle with those of Zubeldia and the applicant's admitted prior art and add the

Oracle Internet Directory service to Zubeldia's system to satisfy the limitation of sending over a secure

10   communication channel for security purposes.

As per claims 9 and 20, the applicant describes the method of creating a CRL as described in

claim 1, which is met by Zubeldia in view of the applicant's admitted prior art, with the following limitation

which is met by Oracle:

15   Storing said CRL in a database accessed via a lightweight directory access protocol (LDAP) that

supports a Secure Sockets Layer (SSL) (Pages 1-3);

Zubeldia in view of the applicant's admitted prior art discloses all the limitations of independent

claim 1. However, neither Zubeldia nor the applicant disclose LDAP or SSL.

Oracle discloses the Oracle Internet Directory, which is a service which uses both SSL (page 3)

20   and LDAP protocol to manage a directory (pages 2-3). SSL provides security and LDAP is "the emerging

standard for directory services" (page 2).

It would have been obvious to one of ordinary skill in the art at the time the invention was filed to

incorporate the ideas of Oracle with those of Zubeldia in view of the applicant's admitted prior art and

incorporate the use of Oracle Internet Directory (and it's use of LDAP and SSL) for directory services and

25   security.

As per claim 22, the applicant describes the limitations of claim 16, which is met by Zubeldia in view of the applicant's admitted prior art, with the additional limitation of an LDAP database. The addition of the database as being LDAP is obvious in view of Oracle for the reasons given in the rejection for claim 9 (see above).

5

As per claim 23, the claim recited the limitation of claim 2, but the claim is rejected by Zubeldia in view of the applicant's admitted prior art in further view of Oracle instead of Zubeldia in view of the applicant's admitted prior art. See the rejection for claim 2.

10

As per claim 24, the claim recited the limitation of claim 3, but the claim is rejected by Zubeldia in view of the applicant's admitted prior art in further view of Oracle instead of Zubeldia in view of the applicant's admitted prior art. See the rejection for claim 3.

Any inquiry concerning this communication or earlier communications from the examiner should

15   be directed to Kevin Schubert whose telephone number is (571) 272-4239. The examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

20   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC)

25   at 866-217-9197 (toll-free).

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER